



CVE-2016-5388

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2016-5388 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-07-19 02:00:00 UTC |
| Updated | 2023-02-12 23:23:00 UTC |
| Description | Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.1 |

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|---|---------|--------|---------|----------|
| Application | Apache | Tomcat | All | All | All | All |
| Application | Apache | Tomcat | All | All | All | All |
| Application | Apache | Tomcat | All | All | All | All |
| Application | Hp | System Management Homepage | All | All | All | All |
| Operating System | Oracle | Linux | 6 | All | All | All |
| Operating System | Oracle | Linux | 7 | All | All | All |
| Operating System | Oracle | Linux | 6 | All | All | All |
| Operating System | Oracle | Linux | 7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node Eus | 7.2 | All | All | All |

| | | | | | | |
|------------------|------------------------|---|-----|-----|-----|-----|
| Operating System | Redhat | Enterprise Linux Hpc Node Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

Reference

Apache Tomcat CVE-2016-5388 Security Bypass Vulnerability

CVE-2016-5388 - Red Hat Customer Portal

Pony Mail!

1353809 – (CVE-2016-5388) CVE-2016-5388 Tomcat: CGI sets environmental variable based on user supplied Proxy request header

Red Hat Customer Portal

Pony Mail!

Red Hat Customer Portal

Vulnerability Note VU#797896 - CGI web servers assign Proxy header values from client requests to internal HTTP_PROXY environment variable

Pony Mail!

Red Hat Customer Portal

Document Display | HPE Support Center

Document Display | HPE Support Center


httpoxy

Apache Tomcat CGI Application "Proxy:" Header Processing Flaw Lets Remote Users Redirect the Target CGI Application Requests to an Arbitrary URL

Document Display | HPE Support Center

Oracle Linux Bulletin - October 2016

Red Hat Customer Portal

| |
|--|
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Red Hat Customer Portal |
| Pony Mail! |
| Red Hat Customer Portal |
| openSUSE-SU-2016:2252-1: moderate: Security update for tomcat |
| Pony Mail! |
| www.apache.org/security/asf-httproxy-response.txt |
| Pony Mail! |
| Pony Mail! |
| [SECURITY] [DLA 1883-1] tomcat8 security update |
| Pony Mail! |
| Pony Mail! |
| Red Hat Customer Portal - Access to 24x7 support and knowledge |
| Red Hat Customer Portal |
| Document Display HPE Support Center |
| Apache Tomcat 7 (7.0.73) - Changelog |
| Oracle Critical Patch Update - July 2017 |
| CVE Program record |
| NVD vulnerability detail |
|  |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

CVE.report and Source URL Uptime Status status.cve.report